View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Electronic Archive of Kyiv Polytechnic Institute

УДК 681.3

ОБНАРУЖЕНИЕ СКРЫТЫХ ВИДЕОКАМЕР

Владислав Галанский*, *Игорь Курдин, Александр Лаврентьев, Михаил Прокофьев
Научно-исследовательский центр «ТЕЗИС» НТУУ «КПИ»

Анотація: **Серед різноманіття атакуючих засобів спецтехніки, в останні роки інтенсивно розвивається техніка схованого спостереження. У цій ситуації стає актуальною розробка і застосування засобів протидії несанкціонованому відеоконтролю, виявлення випромінювань відеозакладок, впроваджених у приміщення об'єкта, і їхня локалізація. Проведено аналіз існуючих засобів сканування і викладені основні концепції створення надійних технічних засобів на прикладі розробленого пристрою**.
Summary: **Among a diversity of attacking means of special engineering last years engineering of latent supervision intensively develops. In this situation there is an actual mining and application of means of counteraction to a unauthorized videoinspection, detection of radiations of videobackfills inserted in puttings of object, and their localization. The analysis of existing means of scanning is conducted and the main concepts of creation of reliable means on an example of the designed device are set**
Ключові слова: **Відеозакладка, відеокамера, моніторинг, електромагнітне поле.**

I Введение

Мировой рынок технических средств несанкционированного получения конфиденциальной информации динамично развивается и по самым скромным подсчетам исчисляется десятками миллиардов долларов. К примеру, по оценкам МВД России сейчас годовой оборот рынка радиоэлектронных средств перехвата информации составляет 1 – 2 млрд. долларов (в 1995 году специалисты оценивали объем российского рынка атакующей спецтехники в 150 – 170 млн. долларов). Такую же картину, в пропорционально меньшем масштабе, можно ожидать и в Украине. Охота за чужими тайнами стала выгодным бизнесом, и не удивительно, что по рентабельности этот вид бизнеса занимает третье место после торговли оружием и наркотиками. И если раньше производство и применение специальных технических средств было исключительно прерогативой государства, то с начала 90-х годов в странах СНГ сформировался и набрал обороты неконтролируемый рынок спецтехники за счет нелегального ввоза из-за рубежа. Несмотря на то, что стоимость отдельных приборов современной профессиональной аппаратуры несанкционированного доступа к информации измеряется десятками тысяч долларов, эта техника нелегально ввозится и используется криминальными и теневыми структурами и негосударственными службами безопасности различных крупных коммерческих компаний.

Следует отметить, что среди многообразия атакующих средств спецтехники в последние годы интенсивно развивается техника скрытого наблюдения. Скрытое наблюдение (дистанционный съем видеоинформации) в силу своей высокой информативности и конспиративности является одним из наиболее перспективных способов получения конфиденциальной информации. Реально противодействовать скрытой видеосъемке крайне сложно, поскольку в большинстве своем установку скрытых видеокамер (видеозакладок) выполняют профессионалы высокого класса, устанавливая миниатюрные видеокамеры типа Pin Hole («булавочное отверстие») не только в стены помещений, но и встраивая их в бытовые предметы: настенные часы, книги, пепельницы. Скрытая видеокамера может быть установлена на обычные телефонные линии, видеокамеры монтируют в телефонных аппаратах. Обнаружить такую камеру невооруженным глазом, особенно при ее камуфлировании, достаточно сложно. Вместе с тем, продажа малогабаритных дешевых видеокамер (30 – 100 $), которые могут быть использованы даже непрофессионалами для скрытого наблюдения, поставили эти устройства по массовости использования в один ряд с радиозакладками («жучками»). То есть то, что раньше было уделом спецслужб – сегодня доступно любому любопытному субъекту.

Сегодня правоохранительные органы и субъекты оперативно-розыскной деятельности снабжаются системами видеонаблюдения для носимого, нательного и объектового внедрения, например, в камуфляже «Блокнот», «Кейс», «Галстук», и приборами TeleObserver 2100 для дистанционного наблюдения в стандартах GSM, PSTN, ISDN.

О возможностях видеокомплексов можно судить по прибору «Eagle Vision», с помощью которого в псевдореальном времени (частота обновления кадра от 6 сек до 1 мин) информация передается по радиоканалу на расстояние до 27 км (www.nelk.ru). А это далеко не самые последние модели зарубежной техники, которую, кстати, благодаря миниатюрному исполнению, довольно легко нелегально ввезти из-за рубежа.

Скрытые видеокамеры (видеозакладки), методы их установки и использования постоянно совершенствуются. Адекватно растет спрос на видеозакладки и совершенствуются их технические характеристики в направлении дальнейшей миниатюризации, повышения скрытности работы и увеличения дальности действия, снижения стоимости. В некоторых случаях в состав комплекта скрытого наблюдения входит также аппаратура дистанционного управления работой видеозакладки. Все это привело к тому, что в последние годы наблюдается устойчивая тенденция вытеснения радиомикрофонов видеозакладками (в состав которых может также входить ауди-модуль) с передачей изображения (и звука) по сети питания или по радиоканалу.

В этой ситуации становится актуальной разработка и применение средств противодействия несанкционированному видеоконтролю, выявление излучений видеозакладок, внедренных в помещения объекта, и их локализация.

II Аппаратура обнаружения видеокамер скрытого наблюдения

Зарубежные эксперты считают, что в мире выявляется только 1 – 2 % шпионской техники, остальная позволяет получить до 60 % всей украденной информации. Эти цифры со всей убедительностью свидетельствуют о неадекватном соответствии профессиональной поисковой аппаратуры и атакующих средств спецтехники. Поэтому на рынке устройств противодействия промышленному и экономическому шпионажу появляются все новые более совершенные средства для поиска каналов утечки информации.

Существует большое количество носимых и настольных приборов для поиска закладных устройств, которые широко используются службами безопасности государственных и коммерческих организаций. Некоторые из них могут быть использованы для поиска скрытых видеокамер.

Как и любой другой работающий электронный прибор скрытую видеокамеру можно обнаружить по радиочастотному излучению ее электронных компонентов. Одним из демаскирующих признаков работающей видеозакладки является наличие в излучаемом ею радиоспектре частот видеосигнала с частотами 50 Гц – 5 МГц. Поэтому для поиска видеозакладок необходимы чувствительные приемники, позволяющие обследовать эфир в этом частотном диапазоне.

К числу таких детекторов-приемников можно отнести, например, широкополосный детектор электромагнитного поля ST 041, комплексы КРОНА-8 и КРОНА-6000М, предназначенные для автоматического обнаружения радиоизлучающих устройств (акустических закладок) и передающих видеокамер и определения их местоположения в контролируемом помещении, поисковый приемник ICOM R-9000.

К числу наиболее совершенных конструкций сканеров радиочастотных излучений можно отнести, например, спектральный коррелятор OSCOR 5000, сочетающий в себе высокочувствительный приемник, спектроанализатор, осциллограф, встроенный микрокомпьютер.

Отдельного внимания заслуживает российская разработка – обнаружитель скрытых видеокамер IRIS VCF-2000, который в последнее время широко рекламируется в специальных изданиях. В отличие от указанных выше приборов для обнаружения различных радиозакладок, данный сканер предназначен только для выявления скрытых видеокамер. На сайте разработчиков (www.iristech.ru), в частности, указывается, что обнаружить скрытую видеокамеру гораздо сложнее других средств съёма информации и до недавнего времени являлось почти невыполнимой задачей, поэтому появление прибора IRIS VCF-2000 явилось сенсацией на рынке технических средств безопасности. По мнению разработчиков этого устройства, ничего подобного на рынке средств безопасности сейчас не существует, поскольку, в отличие от радиозакладок, обнаружить работу скрытой видеокамеры с передачей сигнала по кабелю практически невозможно (за исключением методов нелинейной локации, требующих больших временных затрат).

IRIS VCF-2000 способен обнаруживать работающую миникамеру в радиоспектре 0,5 – 400 МГц в среднем на расстоянии до 4 метров, время обнаружения – до 7 минут. При обследовании объектов большой площади требуется несколько последовательных этапов проверки. Во время поиска рекомендуется выключать находящуюся в помещении электронную бытовую и оргтехнику.

Несмотря на очевидные достоинства, прибор IRIS не лишен существенных недостатков.

1. Как и другие устройства поиска радиозакладок, IRIS работает в широком частотном диапазоне (0,5 – 400 МГц) и, следовательно, в равной степени (как и другие чувствительные приемники) подвержен влиянию эфирных помех, которые в ряде случаев невозможно отделить от полезного сигнала даже при выключении в обследуемом помещении всей бытовой и оргтехники. В результате, как отмечают разработчики, «…индикатор интенсивности иногда неточно указывает местоположение обнаруженного источника», «в некоторых случаях прибор выдает сигнал обнаружения подозрительного источника, при этом в данном помещении видеокамер нет».

2. Разработчики указывают, что устройство IRIS позволяет выявлять *большинство* типов используемых сегодня корпусных и бескорпусных модулей микровидеокамер. Однако один из дилеров (www.sinf.ru), непосредственно реализующий эти устройства, более осторожен и в описании IRIS VCF-2000 отмечает: «Работа бытовых камер и ряда камер охранного назначения не регистрируется». И это можно понять, если учесть, что эти камеры помещены в металлические экраны, существенно уменьшающие интенсивность внешнего излучения в частотном диапазоне 0,5 – 400 МГц. К этому можно добавить, что регистрация прибора также затруднена, если телевизионный сигнал и электропитание передаются по одному коаксиальному кабелю.

Таким образом, разработку прибора IRIS действительно можно признать весьма удачной, однако, из приведенного выше анализа видно, что и эта конструкция не лишена существенных недостатков и ее использование в поисковых мероприятиях не дает гарантии обнаружения видеозакладок в исследуемом помещении.

III Мониторинг низкочастотных излучений видеокамер

По нашему мнению, надежный (гарантированный) поиск экранированных видеозакладок возможен только в низкочастотном спектре 50 (60) Гц – 50 кГц, в котором эффективность экранирования ничтожно мала. И не следует обольщаться тем обстоятельством, что сегодня большинство известных миниатюрных видеозакладок не имеют металлической оболочки. Помещение модуля камеры в простейший металлический экран или монтаж скрытой камеры в конструкционно-строительной арматуре помещения или в металлических элементах приточно-вытяжной вентиляции практически делает ее «невидимой» в спектре высоких радиочастот.

В отличие от большинства других приборов поиска миниатюрных видеокамер, в которых обнаружение паразитных излучений осуществляется в широком спектре радиочастот, был разработан поисковый прибор, с помощью которого осуществляется мониторинг помещения в области низкочастотных магнитных полей. В этом случае становится возможной идентификация видеокамер на низких частотах кадровой и строчной развертки, экранирование которых на данных частотах в миниатюрных конструкциях практически неэффективно. И, следовательно, *любой* скрытый источник излучения, имеющий в своем спектре эти частоты, может быть идентифицирован как видеозакладка.

Разработанный прибор осуществляет перехват слабых низкочастотных радиосигналов в диапазоне частот 50 Гц – 100 кГц. Применение узкополосых фильтров позволило получить высокую чувствительность в исследуемом спектре частот и хороший динамический диапазон. Прибор предназначен для обнаружения и определения местоположения функционирующих видеозакладок и позволяет выявлять видеокамеру на расстоянии до 1 метра.

Прибор имеет встроенный регулятор чувствительности и логарифмическую светодиодную шкалу, а также снабжен тональной идентификацией приближения к видеозакладке.

Конструктивно прибор выполнен в виде компактного носимого модуля с автономным питанием и выносной магнитной антенной, позволяющей выполнять ручное сканирование площади шириной 0,5 метра.

При проведении мониторинга электромагнитных полей в исследуемом помещении с помощью разработанного прибора не требуется отключение электрической и электронной техники. К примеру, прибор мгновенно обнаруживает видеозакладку, расположенную на расстоянии 0,5 метра от работающего телевизора (паразитное излучение которого имеет такие же спектральные характеристики видеосигнала, что и видеокамера, но в сотни тысяч раз превышает его по интенсивности). Таким образом, прибор может успешно использоваться в сложной электромагнитной обстановке (при большом уровне фона) в исследуемом помещении.

УДК 621.318.3.01.

ПРИМЕНЕНИЕ ТОНКИХ МЕТАЛЛИЧЕСКИХ ПЛЕНОК ДЛЯ ЭЛЕКТРОМАГНИТНОГО ЭКРАНИРОВАНИЯ

Александр Борисов, Александр Мачулянский, Михаил Родионов
Национальный технический университет Украины «КПИ»

Аннотация: **Проведен анализ экранов на основе тонких пленок. Рассмотрено использование многослойных пленочных экранов для повышения эффективности экранирования. Приведены экспериментальные данные по эффективности экранирования тонкими пленками.**